

Lab Assignment 6: Preparation

- 1 Keep the network configuration of the machines of **MAQUINA1** and **MAQUINA2** from the previous lab assignment.
- 2 **MAQUINA1** has a container which is running ssh in port 222. Port 222 at local ips of **MAQUINA1** is redirected to the container

```
#!/usr/sbin/nft -f
#en esta maquina la direccion del container es 10.0.3.200
table ip nat {
    chain PREROUTING { #redirigimos conexiones externas alssh al container
        type nat hook prerouting priority dstnat; policy accept;
        ip daddr {192.168.2.10, 192.168.3.10, 192.168.4.10} tcp dport {222} log
        ip daddr {192.168.12.10, 192.168.13.10, 192.168.14.10} tcp dport {222} log
        ip daddr {192.168.2.10, 192.168.3.10, 192.168.4.10} tcp dport {222} dnat to 10.0.3.2
        ip daddr {192.168.12.10, 192.168.13.10, 192.168.14.10} tcp dport {222} dnat to 10.0.
    }
}
```

- 3 Install syslogd in the container (apt-get install inetutils-syslogd)
- 4 create user *hideous* in the container (useradd -m hideous)

Lab Assignment 6: Preparation

Hardening
Operating
Systems
2024/25

- 1 Create rsa keys for user001 user002 and user003 in **MAQUINA2**. user003 should protect his/her with a passphrase.
- 2 Enable user001, user002 and user003 to login into **MAQUINA1** (port 22) from **MAQUINA2** without being asked for a password, although user003 might have to supply the key's passphrase

Lab Assignment 6

Hardening
Operating
Systems
2024/25

- 3 Arrange for user001, user002 and user003 in **MAQUINA2** to log directly into the container of **MAQUINA1** (port 222, using **MAQUINA1** ips) as user *hideous* without being asked for a password, although user003 might have to supply the key's passphrase. Can user001, user002 and user003 from **MAQUINA1** log into the container as user *hideous* without being asked for a password?
- 4 Arrange for the authentication logs of machine **MAQUINA2** to be sent to machine **MAQUINA1** and to file `/dev/tty3` in **MAQUINA2**. Check that it works

NOTE: machine receiving logs has to invoke syslog with the `-r` or `--inet` option, machine sending the logs cannot have syslogd invoked with `--no-forward`. Check `/etc/default/` and syslogd man page

Lab Assignment 6

- 5 Arrange for the authentication logs on machine **MAQUINA2** to be sent ALSO to the container in **MAQUINA1**. Use these three different solutions (do all of them work?)
 - a) **MAQUINA1** sends its authentication logs to the container (with @ip_of_container)
 - b) machine **MAQUINA1** writes its authentication logs to a file in the container
 - c) all traffic from one of **MAQUINA1** IPs is redirected to the container (using nftables) and MAQUINA2 uses this ip to forward its auth logs
- 6 Execute *lynis* program audit **MAQUINA1** and use its output to harden the ssh server at that machine. Allow only user001, user002, user003, user004, user005 and user006 to login using ssh

Lab Assignment 6: Work submission

- After performing the corresponding tasks of the lab assignment, a pdf document, describing what has been done (including screenshots showing the behaviour of the virtual machine, changes made to configuraton files, output from commands. . .) should be sent to
 - `antonio.yanez@udc.es`. (students at udc)
 - `yolanda@det.uvigo.es`. (students at uvigo)
- The subject of the mail should be *FSO: practica-6*
- The attachement should be named with the lab assignment number and the surname and name of the student, in the form `P5-Surname-Name.pdf`, avoiding non-ascii caracteres (á, é, ñ . . .)
 - Example: work submitted by student *Donald Trump Núñez* should come as an attached file named `P5-TrumpNunez-Donald.pdf`
- In the case the lab assignment is made by two students, submit only one copy (named after ONE of the students) and state BOTH names in the pdf document